The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/04/2019

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Firefox versions prior to 69
- Firefox ESR versions prior to 68.1
- Firefox ESR versions prior to 60.9

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Logging-related command line parameters are not properly sanitized when Firefox is launched by another program, such as when a user clicks on malicious links in a chat application. This can be used to write a log file to an arbitrary location such as the Windows 'Startup' folder. Note: this issue only affects Firefox on Windows operating systems. (CVE-2019-11751)
- If a wildcard ('*') is specified for the host in Content Security Policy (CSP) directives, any port or path restriction of the directive will be ignored, leading to CSP directives not being properly applied to content. (CVE-2019-11737)
- An out-of-bounds read vulnerability exists in the Skia graphics library, allowing for the possible leaking of data from memory. (CVE-2019-5849)
- Navigation events were not fully adhering to the W3C's "Navigation-Timing Level 2" draft specification in some instances for the unload event, which restricts access to detailed timing attributes to only be same-origin. This resulted in potential cross-origin information exposure of history through timing side-channel attacks. (CVE-2019-11743)
- WebRTC in Firefox will honor persisted permissions given to sites for access to microphone and camera resources even when in a third-party context. In light of recent high profile vulnerabilities in other software, a decision was made to no longer persist these permissions. This avoids the possibility of trusted WebRTC resources being invisibly embedded in web content and abusing permissions previously given by users. Users will now be prompted for permissions on each use. (CVE-2019-11748)
- Bug showed evidence of memory corruption and is presumed that with enough effort that some of these could be exploited to run arbitrary code (CVE-2019-11735)
- The Mozilla Maintenance Service does not guard against files being hardlinked to another file in the updates directory, allowing for the replacement of local files, including the Maintenance Service executable, which is run with privileged access. Additionally, there was a race condition during checks for junctions and symbolic links by the Maintenance Service, allowing for potential local file and directory manipulation to be undetected in some circumstances. This allows for potential privilege escalation by a user with unprivileged local access. Note: These attacks requires local system access and only affects Windows. Other operating systems are not affected. (CVE-2019-11736)
- If a Content Security Policy (CSP) directive is defined that uses a hash-based source that takes the empty string as input, execution of any javascript: URIs will be allowed. This could allow for malicious JavaScript content to be run, bypassing CSP permissions. (CVE-2019-11738)
- A use-after-free vulnerability can occur while manipulating video elements if the body is freed while still in use. This results in a potentially exploitable crash. (CVE-2019-11746)
- Some HTML elements, such as <title> and <textarea>, can contain literal angle brackets without treating them as markup. It is possible to pass a literal closing tag to .innerHTML on these elements, and subsequent content after that will be parsed as if it were outside the tag. This can lead to XSS if a site does not filter user input as strictly for these elements as it does for other elements. (CVE-2019-11744)
- The "Forget about this site" feature in the History pane is intended to remove all saved user data that indicates a user has visited a site. This includes removing any HTTP Strict Transport Security (HSTS) settings received from sites that use it. Due to a bug, sites on the pre-load list also have their HSTS setting removed. On the next visit to that site if the user specifies an http: URL rather than secure https: they will not be protected by the pre-loaded HSTS setting. After that visit the site's HSTS setting will be restored. (CVE-2019-11747)
- The Firefox installer allows Firefox to be installed to a custom user writable location, leaving it unprotected from manipulation by unprivileged users or malware. If the Mozilla Maintenance Service is manipulated to update this unprotected location and the updated

maintenance service in the unprotected location has been altered, the altered maintenance service can run with elevated privileges during the update process due to a lack of integrity checks. This allows for privilege escalation if the executable has been replaced locally. Note: This attack requires local system access and only affects Windows. Other operating systems are not affected. (CVE-2019-11753)

- Bug showed evidence of memory corruption and is presumed that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2019-11740)
- A vulnerability exists in WebRTC where malicious web content can use probing techniques on the getUserMedia API using constraints to reveal device properties of cameras on the system without triggering a user prompt or notification. This allows for the potential fingerprinting of users. (CVE-2019-11749)
- Bug showed evidence of memory corruption and is presumed that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2019-11734)
- A same-origin policy violation occurs allowing the theft of cross-origin images through a combination of SVG filters and a <canvas> element due to an error in how same-origin policy is applied to cached image content. The resulting same-origin policy violation could allow for data theft. (CVE-2019-11742)
- Given a compromised sandboxed content process due to a separate vulnerability, it is possible to escape that sandbox by loading accounts.firefox.com in that process and forcing a log-in to a malicious Firefox Sync account. Preference settings that disable the sandbox are then synchronized to the local machine and the compromised browser would restart without the sandbox if a crash is triggered. (CVE-2019-9812)
- It is possible to delete an IndexedDB key value and subsequently try to extract it during conversion. This results in a use-after-free and a potentially exploitable crash. (CVE-2019-11752)
- A compromised sandboxed content process can perform a Universal Cross-site Scripting (UXSS) attack on content from any site it can cause to be loaded in the same process. Because addons.mozilla.org and accounts.firefox.com have close ties to the Firefox product, malicious manipulation of these sites within the browser can potentially be used to modify a user's Firefox configuration. These two sites will now be isolated into their own process and not allowed to be loaded in a standard content process. (CVE-2019-11741)
- A type confusion vulnerability exists in Spidermonkey, which results in a non-exploitable crash. (CVE-2019-11750)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the usergrep an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2019-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-26/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-27/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5849
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9812
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11734
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11735
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11737
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11740
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11741
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11742
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11743
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11744
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11746
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11747
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11748
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11749
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11750
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11751
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11752
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11753

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov